

EMAIL SECURITY & CONTINUITY

Cloud Secure Email Gateway

Inspect incoming email.
Keep business moving.

Layered inspection, controlled quarantine and outage queuing for your existing email platform.



**Your mailboxes stay where they are.
SecuraWall adds control to the route.**

securawall.com | Powered by Doz Teknoloji

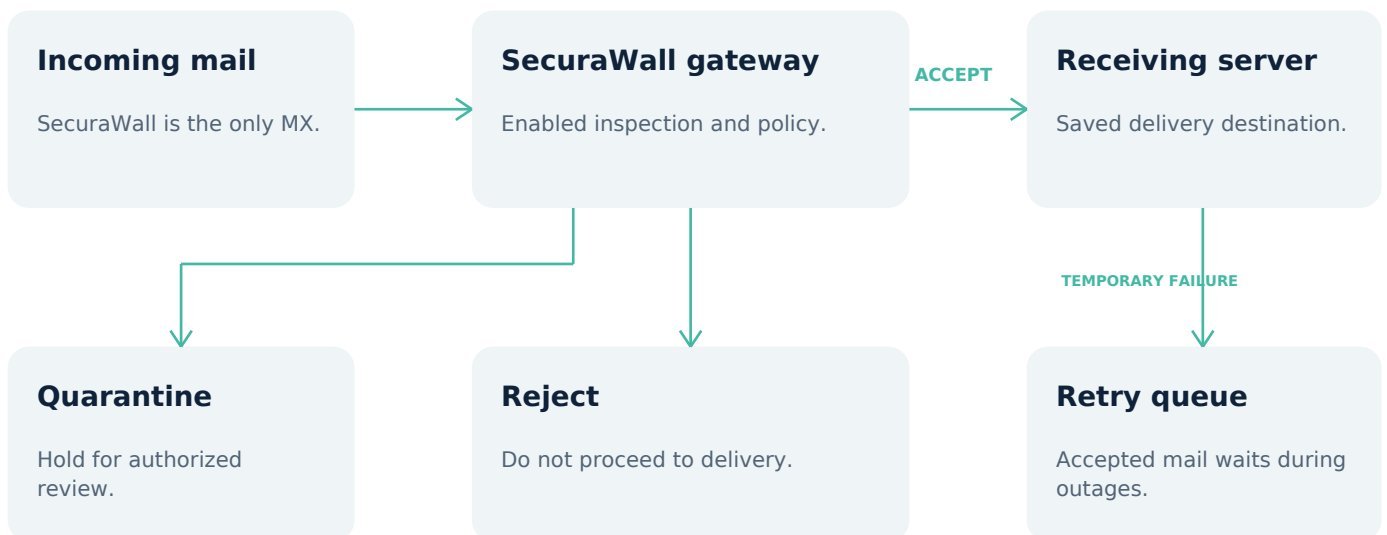
01 / CONTROL THE INCOMING ROUTE

Inspect. Decide. Deliver.

An incoming SMTP gateway for Microsoft 365, Google Workspace, Carbonio and other mail servers. Keep your mailboxes while adding configured inspection and outage queuing; receiving requirements apply.

01	02	03
Reduce exposure	Make review clearer	Support continuity
Apply enabled spam, malware, identity, attachment and link controls before mail reaches your existing platform.	Use recorded reasons and authorized quarantine views to support informed message handling.	Queue accepted messages during temporary destination outages and retry within configured limits.

EMAIL SECURITY / PACKAGE 2



Distinct paths. Quarantine follows a security policy; the retry queue follows a temporary delivery failure. A released message must still pass required checks and reach the destination.

KEEP YOUR MAILBOXES. ADD CONTROL TO THE ROUTE.



02 / LAYERED INSPECTION

Look beyond the subject line.

Configure complementary checks for content, identity and links. Availability depends on the package, enabled policies, scanner readiness and supported formats.

01

Spam & sender authentication

Combine spam scoring with SPF, DKIM and DMARC signals. Domain controls operate within the administrator's global policy.

02

Antivirus & attachment controls

Inspect supported content for malware. Separate filename rules, Office VBA analysis and bounded static ZIP checks inform policy decisions. Static analysis does not execute files.

03

BEC & impersonation signals

Configure protected names and approved senders. Supported lookalike-domain and English/Turkish payment-pressure checks help flag impersonation risk; they do not verify transactions.

04

Click-time link protection

Check supported wrapped links when clicked and again on Continue. Optional Google Web Risk adds URL reputation. Bounded static inspection checks supported redirects and password-form signals. Google receives full checked URLs when enabled; rewriting can affect original DKIM/ARC signatures.

05

QR codes & image text

Extract supported QR content and OCR text from eligible images and the first three PDF pages. Configured blocked-target policies can act on findings; the image scanner does not open extracted URLs.

06

Quarantine & release

IT and personal mailbox views restrict access by authorization. Eligible users can review, release or delete held mail. Release requires a complete fresh antivirus scan.

Coverage matters. Unsupported, encrypted, corrupt or over-limit content may remain partially inspected. Policies can handle incomplete analysis separately. No completed check guarantees that a message, site or sender is safe.



03 / EVERYDAY BUSINESS SCENARIOS

Built around real mail risks.

Put the protection controls in context: payment requests, shared documents and temporary interruptions to the receiving service.

01 An urgent request to change bank details

THE SITUATION	A familiar name asks finance to redirect a payment.
THE CONTROL	Configured BEC checks evaluate supported identity, Reply-To and payment-pressure signals.
THE VALUE	Flag supported risk combinations for policy action. Verify payment changes independently.

02 An invoice arrives with a ZIP or Office file

THE SITUATION	The attachment may contain macros, scripts or content that cannot be fully inspected.
THE CONTROL	Use antivirus, supported VBA and static archive checks, with a separate action for incomplete analysis.
THE VALUE	Apply deliberate message handling and retain the recorded reason for review.

03 The receiving mail server becomes unavailable

THE SITUATION	Maintenance or a temporary network failure interrupts the receiving service.
THE CONTROL	Accepted mail waits in the queue; delivery retries within the configured lifetime.
THE VALUE	Support recovery of incoming mail flow while your existing platform is restored.

Illustrative scenarios, not customer incidents or detection-rate claims. Email inspection cannot authorize a payment, validate every file or guarantee delivery.



04 / OPERATE WITH VISIBILITY

Give each role the right view.

Bring policy management, quarantine review and recorded delivery outcomes into a clear operating workflow.

01

Administrator

Manage global service and security controls within the administrator portal.

02

IT administrator

Manage authorized domains, quarantine users and eligible message actions in the IT portal.

03

Mailbox user

Review eligible held mail for the primary address and authorized aliases; release or delete within current permissions.

Follow each recorded delivery outcome.

Use a Queue ID to connect recorded attempts, SMTP responses, available security decisions and rule contributions. Submission to the local queue, acceptance by the receiving SMTP system and placement in a user inbox are separate outcomes.

Provision quarantine access deliberately.

Create local users manually or review a CSV preview before import. Configured user connections support Google Workspace, Active Directory/LDAP, Carbonio and Zimbra. Connector synchronization and sign-in are separate from SMTP mail routing.

Deploy in three controlled steps

01

Verify

Prove domain ownership and save the real receiving destination.

02

Route

Test the destination, then publish the package-specific MX route.

03

Validate

Test policy, quarantine, outage queuing and the recorded delivery result.

Choose your incoming service.

Select the incoming service for each domain. Add an approved outbound SMTP route when your organization needs it.

Capability	Backup MX	Email Security
Incoming route	Secondary MX	Primary gateway
Outage queuing and retries	Included	Included
Spam and antivirus checks	Not included	Available
Content, BEC and link policies	Not included	Available
Personal quarantine	Not included	Included
SMTP Relay	Optional add-on	Optional add-on

Backup MX stays on standby while the primary is available, then queues eligible incoming mail during outages. Email Security inspects the incoming gateway route and also queues accepted mail during temporary destination failures.

Optional SMTP Relay

Add an authenticated outbound route for the same domain, subject to administrator approval, TLS, verified SPF and applicable quotas. DKIM signing is optional and recommended. The add-on does not add incoming inspection to Backup MX.

Service boundaries

Your mailboxes stay on your current platform. Hosted mailboxes, outage webmail and email archiving are outside this service. Inspection depends on enabled controls and supported analysis limits. Review current settings, retention and message-size limits before deployment.

Plan your email gateway deployment.

securawall.com | proje@dozteknoloji.com | +90 232 332 39 03